

# Acceptable Use Policy

Approved by the Board of Trustees January 24, 2011

Exhibit A: Employee Guidelines for Acceptable Use of Technology Resources

Exhibit B: Student Guidelines for Acceptable Use of Technology Resources

Exhibit C: Agreement for Acceptable Use of the Electronic Communications System by a  
Nonschool User

Exhibit D: Release Form for the Electronic Display of Original Work

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ (LOCAL)  
EXHIBIT A

**Employees Guidelines for Acceptable Use of Technology Resources**

These guidelines are provided here so that employees are aware of the responsibilities they accept when they use district-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMS, digitized information, communication technologies, and internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations
  - a. Use of computers, other technical hardware, computer networks and software is only allowed when granted permission by the employee's supervisor.
  - b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the district website.
  - c. Although the District has an Internet safety plan in place, employees are expected to notify their supervisor or the Executive Director of Technology whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
  - d. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the Executive Director of Technology without discussing it with others.
  - e. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.
  - f. Employees shall be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.
2. Unacceptable Conduct (includes the following, but is not limited to)
  - a. Using the network for illegal activities, including copyright or contract violations, downloading inappropriate materials, viruses, and/or software, to hacking and host file sharing software.
  - b. Using the network for financial or commercial gain, advertising, proselytizing, or political lobbying.

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ (LOCAL)  
EXHIBIT A

- c. Accessing or exploring on-line locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
- d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.
- e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
- f. Wasting finite resources, i.e., downloading movies or music for non-educational purposes.
- g. Gaining unauthorized access anywhere on the network.
- h. Revealing the home address or phone number of one's self or another person.
- i. Invading the privacy of other individuals.
- j. Using another user's account, password, or ID card or allowing another user access to your account, password, or ID.
- k. Coaching, helping, observing or joining any unauthorized activity on the network.
- l. Posting anonymous messages or unlawful information on the system.
- m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning, slanderous.
- n. Falsifying permission, authorization of identification documents.
- o. Obtain copies of, or modify files, data or passwords belonging to other users on the network.
- p. Knowingly placing a computer virus on a computer or network.
- q. Using personal computing devices on the District network, except mobile devices for district approved programs

3. Acceptable Use Guidelines

a. General Guidelines:

- 1. All employees will have access to all available forms of electronic media and communication which is in support of education and

ADOPTED 06/17/02  
UPDATE 88

AMENDED: 11/15/10

January 24, 2011

Page 2 of 5  
Exhibit "A" to  
Resolution No. 10-11-70  
Page 2 of 5

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ (LOCAL)  
EXHIBIT A

research and in support of the educational goals and objectives of the Irving Independent School District.

2. Employees are responsible for their ethical and educational use of the computer on-line services at the Irving Independent School District.
  3. All policies and restrictions of the District's computer on-line services must be followed.
  4. Access to the District's computer on-line services is a privilege and not a right. Each employee will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer on-line services.
  5. The use of any District computer on-line services at the Irving Independent School District must be in support of education and research and in support of the educational goals and objectives of the Irving Independent School District.
  6. When placing, removing, or restricting access to specific databases or other District computer on-line services, school officials shall apply the same criteria of educational suitability used for other education resources.
  7. Transmission of any material which is in violation of any federal or state law is prohibited. This includes, but is not limited to: student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses.
  8. Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual campus administrator or technology administrator will be considered an act of vandalism and subject to disciplinary action in accordance with Board Policy.
- b. Network Etiquette
1. Be polite.
  2. Use appropriate language.
  3. Do not reveal personal data (home address, phone number, and phone numbers of other people).
  4. Remember that the other users of District computer on-line services and other networks are human beings whose culture,

ADOPTED 06/17/02  
UPDATE 88

AMENDED: 11/15/10

January 24, 2011

Page 3 of 5

Exhibit "A" to  
Resolution No. 10-11-70  
Page 3 of 5

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ (LOCAL)  
EXHIBIT A

language, and humor have different points of reference from your own.

5. Users should be polite when forwarding email. The intent of forwarding email should be on a need to know basis.

c. E-Mail

1. E-mail should be primarily used for educational or administrative purposes.
2. E-mail transmissions, stored data, transmitted data, or any other use of District computer on-line services by employees or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.
3. All e-mail and all contents are property of the District.

d. Consequences

The employee, in whose name a system account and/or computer hardware is issued, will be responsible at all times for its appropriate use.

Noncompliance with the guidelines published here in the Student Code of Conduct and in Board Policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the district.

The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications using District equipment and network access is governed by the Texas Open Records Act, therefore, when legally requested, proper authorities will be given access to their content.

**IRVING ISD Acceptable Use Agreement Sheet**

\_\_\_\_\_  
Employee Name (print)

\_\_\_\_\_  
School/Location

I have read the Employee Acceptable Use Guidelines for Irving ISD. I agree to follow the rules contained in these guidelines. I further understand that electronic mail transmissions and other use of the electronic communications systems, including Internet, are not private and may be monitored at any time by the District staff to ensure appropriate use, as defined by the Accepted Use Guidelines. I understand that violations can result in disciplinary action such as denial of access privileges, change in employment status, appropriate legal action and/or termination of employment contract.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

## **Student Guidelines for Acceptable Use of Technology Resources**

These guidelines are provided here so that students and parents are aware of the responsibilities students accept when they use district-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communications technologies and internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

### **1. Expectations**

- a. Student use of computers, other technology hardware, software and computer networks including the internet is only allowed when supervised or granted permission by a staff member.
- b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the district website.
- c. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
- d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

### **2. Unacceptable conduct includes, but is not limited to the following:**

- a. Using the network for illegal activities, including copyright, license or contract violations, downloading inappropriate materials, viruses, and/or software, hacking and host file sharing software.
- b. Using the network for financial or commercial gain, advertising, proselytizing or political lobbying.
- c. Accessing or exploring on-line locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
- d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.
- e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

- f. Wasting finite resources, i.e., downloading movies or music for non-educational purposes.
- g. Gaining unauthorized access anywhere on the network.
- h. Revealing the home address or phone number of one's self or another person.
- i. Invading the privacy of other individuals.
- j. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.
- k. Coaching, helping, observing or joining any unauthorized activity on the network.
- l. Posting anonymous messages or unlawful information on the system.
- m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.
- n. Falsifying permission, authorization or identification documents.
- o. Obtain copies of, or modify files, data or passwords belonging to other users on the network.
- p. Knowingly placing a computer virus on a computer or network.

3. **Acceptable Use Guidelines - Irving Independent School District Network Computer On-Line Services**

a. **General Guidelines**

- (1) Students will have access to all available forms of electronic media and communication which is in support of education and research and in support of the educational goals and objectives of the Irving Independent School District.
- (2) Students are responsible for their ethical and educational use of the computer on-line services at the Irving Independent School District.
- (3) All policies and restrictions of the District's computer on-line services must be followed.
- (4) Access to the Irving Independent School District computer on-line services is a privilege and not a right. Each employee, student



and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer on-line services.

- (5) The use of any District computer on-line services at the Irving Independent School District must be in support of education and research and in support of the educational goals and objectives of the Irving Independent School District.
- (6) When placing, removing, or restricting access to specific databases or other District computer on-line services, school officials shall apply the same criteria of educational suitability used for other education resources.
- (7) Transmission of any material which is in violation of any federal or state law is prohibited. This includes, but is not limited to: confidential information, copyrighted material, threatening or obscene material, and computer viruses.
- (8) Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the IISD Student Code of conduct booklet.
- (9) Any parent wishing to restrict their children's access to any District computer on-line services will provide this restriction request in writing. Parents will assume responsibility for imposing restrictions only on their own children.

**b. Network Etiquette**

- (1) Be polite.
- (2) Use appropriate language.
- (3) Do not reveal data (home address, phone number, phone numbers of other people).
- (4) Remember that the other users of the District's computer on-line services and other networks are human beings whose culture, language, and humor have different points of reference from your own.
- (5) Users should be polite when forwarding email. The intent of forwarding email should be on a need to know basis.

c. **E-Mail**

- (1) E-mail should be used primarily for educational or administrative purposes.
- (2) E-mail transmissions, stored data, transmitted data, or any other use of District computer on-line services by students, employees or other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.
- (3) All e-mail and all contents are property of the District.

4. **Consequences**

The student in whose name a system account and/or computer hardware issued will be responsible at all times for its appropriate use.

Noncompliance with the guidelines published here in the Student Code of Conduct and in Board Policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase III consequence of the Code of Conduct. Violation of applicable state or federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution or disciplinary action by the district.

Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated district staff to ensure appropriate use.

The district cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of email and network communications are governed by the Texas Open Records Act; proper authorities will be given access to their content.

**Irving ISD Acceptable Use Agreement**

**Student Section**

\_\_\_\_\_  
Student name (print)

\_\_\_\_\_  
Grade

\_\_\_\_\_  
School

I have read the Student Acceptable Use Guidelines. I agree to follow the rules contained in this policy. If I violate the rules I may lose my access privilege to the District's computer online services and may face disciplinary action.

\_\_\_\_\_  
Student signature

\_\_\_\_/\_\_\_\_/\_\_\_\_  
Date

**Parent Section**

I have read the Student Acceptable Use Guidelines. I understand that the Internet is a world-wide group of hundreds of thousands of computer networks. I agree that the Irving Independent School District does not control the content of these Internet networks. I understand if my child violates the Acceptable Use Guidelines, his/her access privilege to the District's computer online services may be revoked and may be subject to disciplinary action. The Irving Independent School District has my permission to give network and Internet access to my child. I understand that my child will maintain this privilege as long as the procedures described in the District Acceptable Use Guidelines are followed.

I also grant permission for examples of my child's schoolwork to be published on the World Wide Web as an extension of classroom studies, provided that the home address, home phone number, student's last name or a close-up photograph is not included.

Note: While the District will use filtering technology to restrict objectionable material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use. Parents who do not want their child to have Internet access and/or have their schoolwork published on the web, should submit this request in writing annually to their child's principal. While the district will attempt to restrict access, it is ultimately the responsibility of the parent to ensure their child does not violate this request.

\_\_\_\_\_  
Parent or Guardian signature

\_\_\_\_/\_\_\_\_/\_\_\_\_  
Date

\_\_\_\_\_  
Parent name (print)

\_\_\_\_\_  
Home address

\_\_\_\_\_  
Phone

## AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM BY A NONSCHOOL USER

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

### RULES FOR APPROPRIATE USE

You will be assigned an individual account, and you are responsible for not sharing the password for that account with others.

You will be held responsible at all times for the proper use of your account, and the District may suspend or revoke your access if you violate the rules.

Remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.

#### I. INAPPROPRIATE USES

- a. Using the system for any illegal purpose.
- b. Disabling or attempting to disable any Internet filtering device.
- c. Encrypting communications to avoid security review.
- d. Borrowing someone's account without permission.
- e. Downloading or using copyrighted information without permission from the copyright holder.
- f. Intentionally introducing a virus to the computer system.
- g. Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- h. Wasting school resources through improper use of the computer system.
- i. Gaining unauthorized access to restricted information or resources.

II. CONSEQUENCES FOR INAPPROPRIATE USE

- a. Suspension of access to the system;
- b. Revocation of the computer system account; or
- c. Other legal action, in accordance with applicable laws.

I understand that my computer use is not private and that the District will monitor my activity on the computer system.

I have read the Irving ISD's electronic communications system policy and administrative regulations and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the Irving Independent School District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

Name (Print) \_\_\_\_\_

Signature \_\_\_\_\_

Home address \_\_\_\_\_

Date \_\_\_\_\_ Home phone number \_\_\_\_\_

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

Exhibit III-D  
Page 46  
CQ  
(EXHIBIT D)

EXHIBIT D

RELEASE FORM FOR THE ELECTRONIC DISPLAY OF ORIGINAL WORK

I, \_\_\_\_\_, give my permission for my work to be electronically publicly displayed and produced by the District. The work to be displayed is:

\_\_\_\_\_  
\_\_\_\_\_

Student's or employee's signature \_\_\_\_\_ Date \_\_\_\_\_

Signature of student's parent \_\_\_\_\_

Date \_\_\_\_\_ Home phone number \_\_\_\_\_

DATE ISSUED: 12/11/2009  
UPDATE 88  
CQ(EXHIBIT)-RRM

January 24, 2011

AMENDED: 11/15/2010  
1 of 1

Exhibit "D" to  
Resolution 10-11-70  
Page 1 of 1